STOWELL, THOMAS LEO. Modules over a Principal Ideal Domain. (1974)
Directed by: Dr. Kenneth A. Byrd. Pp. 46

This thesis determines the structure of certain modules over a principal ideal domain, namely the divisible modules and the finitely generated modules. The author proves that any divisible module M over a principal ideal domain D is isomorphic to a direct sum of modules each of which is a copy of the quotient field K_D or to D_{P^∞} for various primes $p \in D$. The author also proves that a finitely generated module is isomorphic to a finite product of cyclic modules. Any finitely generated module is characterized up to isomorphism by certain algebraic invariants. The results on finitely generated modules are then applied to vector space theory to develop the rational and Jordan canonical forms.

MODULES OVER A PRINCIPAL IDEAL DOMAIN

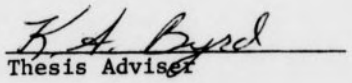
by

Thomas Leo Stowell

A Thesis Submitted to
the Faculty of the Graduate School at
The University of North Carolina at Greensboro
in Partial Fulfillment
of the Requirements for the Degree
Master of Arts

Greensboro
1974

Approved by



Thesis Adviser

APPROVAL SHEET

This thesis has been approved by the following committee of the Faculty of the Graduate School at The University of North Carolina at Greensboro.

Thesis Adviser K. A. Byrd

Oral Examination Committee Members E. E. Posey

Karl Ray Gentry

Andrew F. Long, Jr.

Nov. 15, 1974
Date of Examination

ACKNOWLEDGMENT

The author wishes to express his appreciation to Dr. Kenneth A. Byrd for his assistance in the preparation of this thesis.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION TO MODULES AND PRINCIPAL IDEAL DOMAINS

This first chapter consists mainly of statements and definitions. It is intended to familiarize the reader with modules and principal ideal domains.

Definition: An integral domain D with identity is said to be a principal ideal domain if every ideal I in D is of the form $I = dD = \{ds \mid s \in D\}$ for some d in D.

Examples:

(1) The ring of integers is a principal ideal domain.

(2) $K[x]$ the ring of polynomials in one indeterminate over a field K is a principal ideal domain.

(3) Any euclidean ring is a principal ideal domain .

Definition: Let R be a commutative ring with identity. An element a in R is said to be a unit if there exists an element b in R such that $ab = 1$.

Any element of a principal ideal domain D can be factored using a unit. If $d \in D$ and if $u \in D$ is a unit, then $d = (du^{-1})u$. This is called a trivial factorization.

Definition: A non-zero element x in a ring R is called a prime element if x is not a unit and x has no non-trivial factorization.

Definition: Let R be a commutative ring with identity. Two elements a and b in R are said to be associates if $b = ua$ for some unit u in R.

The relation of being associates is an equivalence relation. Therefore, it splits any commutative ring R with identity into equivalence classes. We can choose a prime, if one exists, from each equivalence class. This set of primes, P, is called a representative collection of primes in R. We have the following:

(1) If r is a non-zero, non-unit element of R. Then $r = up_1 p_2 \cdot \cdot \cdot p_k$ where u is a unit in R and $\{p_i \mid i = 1, \ldots, k\} \subseteq P$.

(2) If r is an element of R such that $r = u_0 p_1 p_2 \cdot \cdot \cdot p_k = u_1 q_1 q_2 \cdot \cdot \cdot q_s$ where u_0 and u_1 are units in R and where $\{p_i \mid i = 1, \ldots, k\}$ and $\{q_j \mid j = 1, \ldots, s\}$ are subsets of P. Then, $u_0 = u_1$, $k = s$, and the q_j's can be renumbered so that $p_1 = q_1$, $p_2 = q_2$, etc.

Let D be a principal ideal domain, let $a|b$ read "a divides b" if and only if $b = ad$ for some $d \in D$. There is a meaningful relation between $\subseteq$ (containment) of ideals and $|$ (divides) among elements in D.

(1) $aD \subseteq bd$ if and only if $b|a$

(2) $aD = bD$ if and only if a and b are associates.

In a principal ideal domain every statement about divisibility can be rewritten as a statement about ideals and containment and vice-versa.

Example:

Given two elements a and b in D, we say $d \in D$ is a greatest common divisor of a and b if and only if:

(1) $d|a$ and $d|b$

(2) if $k|a$ and $k|b$ then $k|d$.

This translates to:

(1) $aD \subseteq dD$ and $bD \subseteq dD$

(2) if $aD \subseteq kD$ and $bD \subseteq kD$ then $dD \subseteq kD$.

Notice dD contains both aD and bD and is the smallest such ideal therefore $dD = aD + bD = \{ax + by \mid x, y \in D\}$.

Definition: In a principal ideal domain D, d is a greatest common divisor of a and b if $aD + bD = dD$ for $a, b, d \in D$. For short we denote this relationship by $(a,b) = d$.

From this point on, D will denote a principal ideal domain and P will denote a representative collection of primes in D.

Definition: Let R be a ring with identity 1. A non-empty set M is said to be a right R-module, denoted M_R, if M is an abelian group under $+$, and for every $r \in R$, $m \in M$, there exists an element mr in M so that the following conditions hold:

(1) $(a + b)r = ar + br$

(2) $(as)r = a(sr)$

(3) $a(r + s) = ar + as$

(4) $(a)1 = a$

for all $a, b \in M$ and $r, s \in R$.

Examples:

(1) Every abelian group G is a module over the ring of integers.

(2) Any ring R is a module over itself denoted R_R.

(3) Let R be a ring. Let I be any ideal of R. Then $\frac{R}{I}$ is an R-module.

From this point on, M_D will denote a module over a principal ideal domain D and M_R will denote a module over a ring R with identity 1.

Definition: A module M_R is said to be cyclic if there exists an element m_0 in M such that every $m \in M$ is of the form $m = m_0 r$. We then write $M = m_0 R$ and we say that m_0 generates M.

Theorem 1.1: A cyclic module $M_D = m_0 D$ is isomorphic to $\frac{D}{d_0 D}$ where $d_0 D = \{d \in D \mid m_0 d = 0\}$.

Proof: Let $\phi: D \to M$ be defined by $\phi(d) = m_0 d$. Then ϕ is an epimorphism and by the first isomorphism theorem, $M \cong \frac{D}{\text{Ker } \phi}$ but $\text{Ker } \phi = \{d \in D \mid m_0 d = 0\} = d_0 D$. Hence $M \cong \frac{D}{d_0 D}$.

Theorem 1.2: If d is a non-zero element of D and if $d = u p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ for some unit u and $\{p_i \mid i = 1, \ldots, k\} \subseteq P$ then $\frac{D}{dD} \cong \frac{D}{p_1^{n_1} D} \times \frac{D}{p_2^{n_2} D} \times \cdots \times \frac{D}{p_k^{n_k} D}$.

Proof: Let $\phi: D \to \coprod_{i=1}^{k} \frac{D}{p_i^{n_i} D}$ be defined by $\phi(x) = (x + p_1^{n_1} D, x + p_2^{n_2} D, \ldots, x + p_k^{n_k} D)$. Then we have the following:

$$(1)\quad \phi(x+y) = (x+y+p_1{}^{n_1}D, x+y+p_2{}^{n_2}D, \ldots, x+y+p_k{}^{n_k}D)$$

$$= (x+p_1{}^{n_1}D, x+p_2{}^{n_2}D, \ldots, x+p_k{}^{n_k}D) + (y+p_1{}^{n_1}D, y+p_2{}^{n_2}D, \ldots, y+p_k{}^{n_k}D)$$

$$= \phi(x)+\phi(y)$$

$$(2)\quad \phi(xr) = (xr+p_1{}^{n_1}D, xr+p_2{}^{n_2}D, \ldots, xr+p_k{}^{n_k}D)$$

$$= (x+p_1{}^{n_1}D, x+p_2{}^{n_2}D, \ldots, x+p_k{}^{n_k}D)r$$

$$= [\phi(x)]r \quad \text{for} \quad r \in D.$$

We see from (1) and (2) that ϕ is an R-homomorphism.

Let $y \in \prod_{i=1}^{k} \frac{D}{p_i{}^{n_i}D}$. Then for some $d_i \in D$ we have

$$y = (d_1+p_1{}^{n_1}D, d_2+p_2{}^{n_2}D, \ldots, d_k+p_k{}^{n_k}D)$$

$$= (d_1+p_1{}^{n_1}D, 0, \ldots\ \ldots, 0)$$

$$+ (0, d_2+p_2{}^{n_2}D, 0, \ldots\ \ldots, 0)$$

$$+$$

$$\vdots$$

$$+ (0, \ldots\ \ldots, 0, d_k+p_k{}^{n_k}D)$$

Looking at one summand at a time, I claim I can find a $d_i'' \in D$ so that $\phi(d_i'') = (0,\ldots,0,1+p_i{}^{n_i}D,0,\ldots,0)$. Let $d_i' = p_1{}^{n_1}\cdots p_{i-1}{}^{n_{i-1}}\, p_{i+1}{}^{n_{i+1}}\cdots p_k{}^{n_k}$ then d_i' and $p_i{}^{n_i}$ are relatively prime so there exists elements s_i and r_i in D so that $d_i' r_i + p_i{}^{n_i} s_i = 1$. Hence $\phi(d_i' r_i) = (0,\ldots,0,1+p_i{}^{n_i}D,0,\ldots,0)$ Letting $d_i'' = d_i' r_i$, then $\phi(d_i d_i'') = (0,\ldots,0,d_i+p_i{}^{n_i}D,0,\ldots,0)$. We can repeat this procedure for each summand. Hence $\phi(\sum d_i d_i'') = y$.

This tells us ϕ is onto. So, by the first isomorphism theorem, $\prod_{i=1}^{k} \frac{D}{p_i^{n_i}D} \cong \frac{D}{\text{Ker } \phi}$. But Ker ϕ = dD.

Subproof: i) Let $x \in dD$. Then $x = dr$ for some $r \in D$.

$$\phi(x)=\phi(dr)=(dr+p_1^{n_1}D, dr+p_2^{n_2}D, \ldots, dr+p_k^{n_k}D)$$

$$=(0+p_1^{n_1}D, 0+p_2^{n_2}D, \ldots, 0+p_k^{n_k}D) = \bar{0}.$$

Hence $dD \subseteq \text{Ker } \phi$.

ii) Let $x \in \text{Ker } \phi$. Then

$$\phi(x) = (x+p_1^{n_1}D, x+p_2^{n_2}D, \ldots, x+p_k^{n_k}D) = \bar{0}$$

which implies $x \in \bigcap_{i=1}^{k} p_i^{n_i}D$. Hence $x \in p_1^{n_1}\ldots p_k^{n_k}D = dD$. Hence Ker $\phi \subseteq dD$. Therefore, $\prod_{i=1}^{k} \frac{D}{p_i^{n_i}D} \cong \frac{D}{dD}$.

Definition: A module M is said to be noetherian if it has the ascending chain condition on submodules, i.e., M has no infinite strictly increasing sequence of submodules.

Definition: A module M is said to be artinian if it has the descending chain condition on submodules.

An important property of a noetherian module is that any non-empty set of submodules has a maximal member.

Theorem 1.3: Every principal ideal domain D is a noetherian ring. i.e., D_D is noetherian.

Proof: Given any chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$, then $\bigcup_{i=1}^{\infty} I_i$ is an ideal in D. If x generates $\bigcup_{i=1}^{\infty} I_i$, then $x \in I_n$ for some n. But then, $xD \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$, hence $I_n = I_{n+1} = \cdots$.

Theorem 1.4: If d is a non-zero element of D then $\frac{D}{dD}$ is a noetherian and artinian D-module.

Proof: Every submodule of $\frac{D}{dD}$ is of the form $\frac{A}{dD}$ where A is a D-module and $dD \subseteq A \subseteq D$. There are only a finite number of these for if $up^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ represents the prime decomposition of d, then the submodule A is of the form $p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} D$ where $r_i \leq n_i$ for $i = 1,2,\ldots, k$, and there are only a finite number of these arrangements. So, every chain of submodules of $\frac{D}{dD}$ is finite therefore $\frac{D}{dD}$ satisfies the descending and ascending chain conditions. Hence $\frac{D}{dD}$ is an artinian and noetherian D-module.

Definition: A non-zero module is said to be indecomposable if it is not isomorphic to the direct product of two non-zero modules.

Example:

For $p \in P$, $\frac{D}{p^k D}$ is an indecomposable D-module.

Krull-Schmidt Theorem: Let M be an artinian and noetherian module. If $M \cong K_1 \oplus K_2 \oplus \cdots \oplus K_n$ where the K_i, $i = 1, \ldots, n$ are non-zero indecomposable modules and $M \cong L_1 \oplus L_2 \oplus \cdots \oplus L_m$ where the L_j, $j = 1, \ldots, m$ are non-zero indecomposable modules. Then $m = n$ and with appropriate indexing $K_i \cong L_i$.

The Krull-Schmidt Theorem tells us that the decomposition of $\frac{D}{dD}$ in Theorem 1.2 is unique up to indexing.

We conclude this chapter with its most important example. Given a prime element p in a principal ideal domain D, if K is the quotient field of D then we define $D_{p^\infty} = \left(\frac{K}{D}\right)_{(p)} = \{\frac{a}{b} + D \mid b = p^n \text{ for some } n \geq 0\}$. D_{p^∞} has the property

that each of its elements is annihilated by a non-negative power of p.

We shall denote the coset $(\frac{a}{b} + D)$ by $\frac{\bar{a}}{b}$. All proper submodules of D_p^∞ are cyclic submodules of the form $H_k = \{\frac{\bar{a}}{p^k} \mid a \in D\}$ where $\frac{\bar{1}}{p^k}$ generates H_k.

Proof: We have the sequence $0 = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_i \subset \ldots$ of submodules of D_p^∞. $D_p^\infty = \bigcup_{i=0}^{\infty} H_i$. We want to show that these are the only proper submodules of D_p^∞. Assume H is a proper submodule of D_p^∞ such that $H \neq H_k$ for every $k \geq 0$. Let n be the first integer such that $H_n \nsubseteq H$ but $H_{n-1} \subseteq H$. I claim $H = H_{n-1}$.

Subproof: Assume $H \neq H_{n-1}$, then there exists an element $\frac{\bar{a}}{p^k}$ in $H - H_{n-1}$. Note that $k \geq n$ else $\frac{\bar{a}}{p^k} \in H_{n-1}$. We may assume $(a,p^n) = 1$, so $(a,p) = 1$ and there exists elements r and s in D such that $ar + ps = 1$. Therefore, $\frac{\bar{1}}{p^k} = \frac{\overline{ar}}{p^k} + \frac{\overline{ps}}{p^k}$, and if $k = n$, then $\frac{\overline{ps}}{p^k} = \frac{\overline{ps}}{p^n} = \frac{\bar{s}}{p^{n-1}} \in H_{n-1}$ hence $\frac{\bar{1}}{p^n} \in H$ which is a contradiction. If $k > n$, then $k - n = j > 0$. So, $p^j(\frac{\bar{1}}{p^k}) = p^j(\frac{\overline{ar}}{p^k} + \frac{\overline{ps}}{p^k})$ which implies $\frac{\bar{1}}{p^n} = \frac{\overline{ar}}{p^n} + \frac{\overline{ps}}{p^n}$ and since $\frac{\overline{ar}}{p^k} \in H$, $\frac{\overline{ar}}{p^n} = \frac{\overline{ar}}{p^{k-j}} \in H$ and $\frac{\overline{ps}}{p^n} = \frac{\bar{s}}{p^{n-1}} \in H$ so $\frac{\bar{1}}{p^n} \in H$ which is a contradiction. Therefore, containment is not proper hence $H = H_{n-1}$. This completes our proof.

We later show that D_p^∞ has the important property of being <u>divisible</u> as a D-module.

CHAPTER II

DIVISIBLE MODULES

Unless otherwise specified, all modules mentioned in the following chapters will be over principal ideal domains.

Definition: If each of the elements x of a module M_D has a non-zero annihilator, i.e., ann $x = \{d \in D \mid xd = 0\} \neq 0$ then we say that M_D is a torsion module.

Definition: If each of the non-zero elements of a module M_D has zero annihilator, then we say that M_D is a torsion-free module

For any arbitrary module M_D we can look at the set of all elements in M_D which have non-zero annihilators. We can call this set tM. Then tM is a submodule of M_D.

Proof: (1) Let m_1 and m_2 be elements of tM. There exists non-zero elements d_1 and d_2 in D so that $m_1d_1 = m_2d_2 = 0$. $(m_1 + m_2)d_1d_2 = m_1d_1d_2 + m_2d_1d_2 = (m_1d_1)d_2 + (m_2d_2)d_1 = 0$. Therefore, $(m_1 + m_2)$ is an element of tM.

(2) Let m be an element of tM. There exists a non-zero element d in D so that $md = 0$. $(mr)d = m(rd) = m(dr) = (md)r = 0$ for any r in D. Therefore, mr is an element of tM.

The module $\frac{M}{tM}$ is torsion-free.

Proof: Let $m + tM$ be an element of $\frac{M}{tM}$. If $m \in tM$, then $m + tM = \bar{0}$. If $m \notin tM$, then ann $m = 0$. I claim ann $(m + tM) = 0$. Suppose $(m + tM)d = \bar{0}$ where ann $m = 0$, then $md + tM = \bar{0}$.

i.e., $md \in tM$. This means there is a non-zero $d_1 \in D$ so that $(md)d_1 = 0$. Since ann $m = 0$, then $dd_1 = 0$, and since $d_1 \neq 0$, then $d = 0$. Therefore, ann $(m + tM) = 0$ and $\frac{M}{tM}$ is torsion-free.

Definition: A module M_D is said to be p-primary if every element in M_D is annihilated by some power of p where $p \in P$.

Theorem 2.1: Any torsion module M_D is the direct sum of p-primary submodules.

Proof: For every prime ideal pD, $p \in P$, we define $M_{(p)}$ to represent the set of all elements of M_D which have annihilator a power of p.

$M_{(p)}$ is a submodule of M_D.

Subproof: (1) Let m_1 and m_2 be elements of $M_{(p)}$. There exists non-negative integers r and s so that $m_1p^r = m_2p^s = 0$. $(m_1 + m_2)p^{r+s} = m_1p^{r+s} + m_2p^{r+s} = m_1p^{r+s} + m_2p^{s+r} = 0$. Therefore, $(m_1 + m_2)$ is an element of $M_{(p)}$.

(2) Let m be an element of $M_{(p)}$. There exists an non-negative integer n so that $mp^n = 0$.
$(mr)p^n = m(rp^n) = m(p^nr) = (mp^n)r = 0$ for any r in D. Therefore, mr is an element of $M_{(p)}$.

$M_D = \bigoplus_{p \in P} M_{(p)}$.

Subproof: (1) Let x be any element of M_D and suppose $xn = 0$ where $n \in D$, $n \neq 0$. Since n is an element of D, n can be factored into primes. $n = up_1^{r_1}p_2^{r_2} \cdots p_k^{r_k}$, where u is a unit and $p_i \in P$, $i = 1,2, \ldots, k$. Let $n_i = \frac{n}{p_i^{r_1}}$, for $i = 1, 2, \ldots, k$;

then the set of elements $n_1, n_2, \ldots, n_k$ are all relatively prime. Therefore, $n_1D + n_2D + \ldots + n_kD = D$ and there exist elements $a_1, a_2, \ldots, a_k$ in D so that $a_1n_1 + a_2n_2 + \ldots a_kn_k = 1$. Multiplying both sides by x we get

$a_1n_1x + a_2n_2x + \ldots + a_kn_kx = x$, where ann $n_ix = p_i^{n_i}D$ so $n_ix \in M_{(p_i)}$.

Let $x = \sum m_i = 0$ where each $m_i \in M_{(p_i)}$, then $m_i = \sum_{j \neq i} (-m_j)$. Let ann $m_i = p_i^{s_i}D$, then ann $m_i \supseteq \bigcap_{j \neq i}$ ann m_j. Hence, $p_i^{s_i}D \supseteq \bigcap_{j \neq i} p_j^{s_j}D \supseteq (\prod_{j \neq i} p_j^{s_j})D$. This implies $p_i^{s_i} \Big| \prod_{j \neq i} p_j^{s_j}$ so $s_i = 0$ and ann $m_i = D$, therefore $m_i = 0$. We thus have independence, Hence $M = \bigoplus_{p \in P} M_{(p)}$.

Two examples of Theorem 2.1 are the following:

(1) Let $G = \frac{Z}{12Z}$. G is a torsion cyclic Z-module.

$G = \{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6},\overline{7},\overline{8},\overline{9},\overline{10},\overline{11}\}$. $12\text{-}2^2.3$.

Then $G_{(2)} = \{\overline{0},\overline{3},\overline{6},\overline{9}\} \cong \frac{Z}{4Z}$

$G_{(3)} = \{\overline{0},\overline{4},\overline{8}\} \cong \frac{Z}{3Z}$

and $G = G_{(2)} \oplus G_{(3)} \cong \frac{Z}{3Z} \times \frac{Z}{4Z}$

(2) Consider the torsion Z-module $\frac{Q}{Z}$ (rationals mod one).

Then $\frac{Q}{Z} = \bigoplus_{p \in P} Z_{p^\infty}$. i.e., $(\frac{Q}{Z})_{(p)} = Z_{p^\infty}$.

Definition: A module M_D is said to be divisible if for every x in M_D and every non-zero $d \in D$, there is an element y in M_D so that $x = yd$.

One notices that a non-zero cylcic module M_D is not divisible, unless D is a field. Also, the direct sum of non-zero cylcic modules

is not divisible. As a matter of fact, a direct sum of modules is divisible if and only if each summand is divisible.

Proof: ($\rightarrow$) Let M_D be a divisible module such that $M = \bigoplus_{i\in I} M_i$. Let $x_0 \in M_{i_0}$. Let d be a non-zero element of D. Since M_{i_0} is a submodule of M, and since M is divisible, there is a y in M so that $x_0 = yd$. Let $y = \sum_{i\in I} m_i$, then $x_0 = (\sum_{i\in I} m_i)d$. Now $M = \bigoplus_{i\in I} M_i$ so $m_i d \neq 0$ unless $i = i_0$. Hence $x_{i_0} = m_{i_0} d$ where $m_{i_0} \in M_{i_0}$ so M_{i_0} is a divisible submodule of M.

($\leftarrow$) Let each summand of M_D be divisible. If x is an element of M_D, then $x = \sum m_i$, and if d is a non-zero element of D, $x = \sum m_i' d$ where $m_i' d = m_i$, $m_i' \in M_i$. Hence $x = m_i' d = (m_i')d = yd$ where $y = \sum m_i'$. This shows that M_D is a divisible module.

It is well known that a homomorphic image of a divisible module is divisible. The proof of this statement is straightforward and will be omitted.

Example:

Let K be the quotient field of D. Let p be a prime in D. Then there is an epimorphism $\phi: K \rightarrow \frac{K}{D}$, and an epimorphism $\psi: \frac{K}{D} \rightarrow \frac{K}{D_{(p)}}$. Therefore $D_{p^\infty} = \frac{K}{D_{(p)}}$ is a homomorphic image of K. Hence D_{p^∞} is a divisible D-module.

Theorem 2.2: A divisible submodule of a module M_D is a direct summand.

Proof: Let H be a divisible submodule of M. Our objective is to find a submodule K such that $M = H \oplus K$. Consider the set B of all submodules L, such that $H \cap L = 0$. B contains the zero module

hence is non-empty. B can be partially ordered by set inclusion. Let $\{L_i\}$ be any chain in B and let J be the set theoretic union of L_i's. Then:

1) J is a submodule of M.

Subproof: i) Let j_1 and j_2 be elements of J. Then $j_1 \in L_i$ and $j_2 \in L_k$ for some i and k. Therefore either $(j_1 + j_2) \in L_i$ or $(j_1 + j_2) \in L_k$. Hence $(j_1 + j_2) \in J$.

ii) Let j be an element of J. Then $j \in L_i$ for some i. Hence $jr \in L_i$ for any $r \in D$, therefore $jr \in J$.

2) $H \cap J = 0$.

Subproof: Every element of J is an element of some L_i and $H \cap L_i = 0$. Therefore, $H \cap J = 0$.

3) J is an upper bound of $\{L_i\}$ in B.

So by Zorn's Lemma, B has maximal elements. Let K be one of these. I claim $m + H \oplus K$. Suppose $M \neq M \oplus K$, then there is an x in M not in $H \oplus K$. We can, therefore, form the module $K' = K + xD$. By the maximality of K, $H \cap K' \neq 0$, so there is a non-zero element h in $H \cap K'$, $h = k + xd$ for some non-zero d in D, therefore $xd = h - k$ is an element of $H+K$. We may consider the ideal $\{d \in D \mid xd \in H+K\}$. This is a non-zero ideal, so we may suppose that it is generated by an element n in D, $nD = \{d \in D \mid xd \in H+K\}$, n is not a unit else $x = 0$ which is a contradiction. So, nD is a non-zero proper ideal. Therefore, there is a prime p such that $n = pm$ for some $m \in D$.

Let $y = xm$, then y is not an element of $H+K$ but $yp = xmp = xn$ is. So, $yp = h_1 + k_1 = h_2 p + k_1$ because of the divisibility of H. Let $z = y - h_2$, then z is not an element of $H+K$, but $zp = (y - h_2)p = yp - h_2p = h_1 + k_1 - h_2p = h_2p + k_1 - h_2p = k_1$ is in K. So, if $M \neq H+K$, i.e., $M \supset H+K$, then there is a $z \in M$, $z \notin H+K$ and a prime p so that the ideal $\{d \in D \mid zd \in K\} = pD$. Now, $\{d \in D \mid zd \in H+K\} = \{d \in D \mid yd \in H+K\} = \{d \in D \mid zd \in K\} = pD$. Consider $K + zD \supset K$, then $H \cap (K + zD) \neq 0$ and there is a $k_0 \in K$, a non-zero $d_0 \in D$, and non-zero $h_0 \in H$, so that $k_0 + zd_0 = h_0$. Therefore, $d_0 \in \{d \in D \mid zd \in H+K\} = \{d \in D \mid zd \in K\} = pD$. Hence $d_0 \in pD$ and $d_0 = p\ell$ for some $\ell \in D$. But this implies $zd_0 \in K$, and therefore $h_0 \in K$, which implies $H \cap K \neq 0$. This contradiction tells us that no x exists so that $x \in M$, $x \notin H+K$. Hence, $M = H+K$ and, by property 2, $H \cap K = 0$ so our sum is direct. Our proof is complete, $M = H \oplus K$.

Theorem 2.3: Any module M_D has a unique largest divisible submodule H, so that $M = H \oplus K$ where K has no divisible submodules.

Proof: Let $\{H_i \mid i \in I\}$ be the set of divisible submodules of M. Let $H = \sum_{i \in I} H_i$, then H is a divisible submodule of M_D.

Subproof: Let h be an element of H. Let d be a non-zero element of D, then $h = \sum h_i = \sum h_i' d = (\sum h_i')\, d = h'd$ where $h' = \sum h_i'$ and $h_i' d = h_i$. Hence H is divisible.

Now, H contains every divisible submodule H_i, so H is the largest divisible submodule of M_D and hence unique. And, by Theorem 2.2, $M = H \oplus K$, in this case K can have no non-zero divisible submodules for they would be contained in H. This completes our proof.

One interesting point is that H is unique because it is the largest divisible submodule of M. K is not necessarily unique. However, $K \cong \frac{M}{H}$, hence K is unique up to isomorphism.

Example:

Let $M = Q \times Z$. By Theorem 2.3, M has a largest divisible submodule H and $M = H \oplus K$ where K has no divisible submodules. Well, $H = Q \times 0$ and $M = H \oplus K$ where $K = 0 \times Z$ and also $M = H \oplus K'$ where $K' = \{(a,a) \mid a \in Z\}$.

Lemma 2.4: If R_D is a non-zero, p-primary, divisible D-module, then R_D contains a copy of D_{p^∞}.

Proof: Choose in R_D an element x_1 with annihilator pD. Such an x_1 exists, for if x is a non-zero element in R_D, there is a least positive integer k so that $xp^k = 0$ and xp^{k-1} is our desired x_1. Because of the divisibility of R_D, there is an $x_2 \in R_D$ so that $x_1 = x_2 p$. Continuing, there is an $x_3 \in R_D$ so that $x_2 = x_3 p$, and in general, there is an $x_{i+1} \in R_D$ such that $x_i = x_{i+1} p$. Then ann $x_i = p^i D$. Let R_D' be the submodule of R_D generated by $\{x_1, x_2, \ldots\}$. We can construct an isomorphism between this module and D_{p^∞}. Let $\phi: R_D' \to D_{p^\infty}$ be defined by $\phi(\sum x_i d_i) = \sum \bar{1}_{p^i} d_i$.

1) Let $\sum_{i=1}^{n} x_i d_i = \sum_{i=1}^{n} x_i d_i'$. Then $\sum_{i=1}^{n} x_i d_0'' = 0$ where $d_i'' = (d_i - d_i')$. And because $x_i = x_n p^{n-i}$ for $i = 1, \ldots, n$ we get

$$x_n p^{n-1} d_1'' + x_n p^{n-2} d_2'' + \ldots + x_n p d_{n-1}'' + x_n d_n'' = 0$$

$$x_n (p^{n-1} d_1'' + p^{n-2} d_2'' + \ldots + p d_{n-1}'' + d_n'') = 0.$$

Since ann $x_n = p^n D$, this is equivalent to saying that

$$p^n \mid (p^{n-1}d_1'' + p^{n-2}d_2'' + \ldots + pd_{n-1}'' + d_n'').$$

For $\phi(\sum x_i d_i'') = \bar{0}$ means $\frac{\bar{1}}{p}d_1'' + \frac{\bar{1}}{p^2}d_2'' + \ldots + \frac{\bar{1}}{p^n}d_n'' = \bar{0}$.

This is equivalent to

$$\frac{\overline{p^{n-1}}}{p^n}\, d_1'' + \frac{\overline{p^{n-2}}}{p^n}\, d_2'' + \ldots + \frac{\bar{p}}{p^n}\, d_{n-1}'' + \frac{\bar{1}}{p}\, d_n'' = \bar{0}.$$

Which is equivalent to

$$p^n \mid (p^{n-1}d_1'' + p^{n-2}d_2'' + \ldots + pd_{n-1}'' + d_n'').$$

So we have the same conditions on $\phi(\sum x_i d_i'') = \bar{0}$ as for $\sum x_i d_i'' = \bar{0}$. Hence $\phi(\sum x_i d_i'') = \bar{0}$ if and only if $\sum x_i d_i'' = 0$. So, if $\sum x_i d_i = \sum x_i d_i'$, then $\sum x_i (d_i - d_i') = 0$, which implies $\phi(\sum x_i (d_i - d_i') = \bar{0}$, which implies $\phi(\sum x_i d_i) - \phi(\sum x_i d_i') = \bar{0}$ which implies $\phi(\sum x_i d_i) = \phi(\sum x_i d_i')$. Hence ϕ is a well-defined mapping.

2) Let z and w be elements of R_D' with $z = \sum x_i d_i$ and $w = \sum x_i d_i'$. Then

$$\begin{aligned}\phi(z + w) &= \phi[\textstyle\sum x_i d_i + \sum x_i d_i'] \\ &= \phi(\textstyle\sum x_i (d_i + d_i')) \\ &= \textstyle\sum \frac{\bar{1}}{p_i}(d_i + d_i') = \sum \frac{\bar{1}}{p_i} d_i + \sum \frac{\bar{1}}{p_i} d_i' \\ &= \phi(z) + \phi(w).\end{aligned}$$

And

$$\begin{aligned}\phi(zr) &= \phi(\textstyle\sum x_i d_i r) \\ &= \textstyle\sum \frac{\bar{1}}{p_i} d_i r = (\sum \frac{\bar{1}}{p_i} d_i) r = \phi(z) r\end{aligned}$$

for any $r \in D$. Hence ϕ is a homomorphism.

3) If $\phi(\sum x_i d_i'') = \bar{0}$ then $\sum x_i d_i'' = 0$. This was shown in part 1. Hence ϕ is one-to-one.

4) The set $\{\frac{\bar{1}}{p_i} \mid i = 1, 2, \ldots\}$ generates D_p^{∞}. So for a given element d in D_p^{∞} there exists d_i's so that $d = \sum \frac{\bar{1}}{p_i} d_i$. But, $d = \sum \frac{\bar{1}}{p_i} d_i = \phi(\sum x_i d_i)$. Therefore every $d \in D_p^{\infty}$ is in the image of ϕ. Hence ϕ is onto. This completes the proof of our lemma.

Theorem 2.5: A divisible module M_D is a direct sum of modules each isomorphic to K (the quotient field of D) or to D_p^{∞} for various primes p.

Proof: Let T_D be the torsion submodule of M_D. T_D is a divisible module.

Subproof: Let t be an element of T. We want to show if d is a non-zero element of D there is a $t_1 \in T$ so that $t = t_1 d$. Since M is a divisible module, we know there is a $t_1 \in M$ so that $t = t_1 d$. We need only show that $t_1 \in T$. Now, if $t \in T$ there is a non-zero $d_0 \in D$ so that $td_0 = 0$. So $(t_1 d)d_0 = 0$ where $dd_0 \neq 0$. Hence t_1 is an element of T.

By Theorem 2.2, $M = T \oplus F$ where F is isomorphic to $\frac{M}{T}$. Hence F is divisible and torsion free. The study of M can be broken into the study of T and F separately.

We shall study F first. Let x be an element of F. Let r be a non-zero element of D. Since F is divisible and torsion-free there is exactly one element y in F such that $x = yr$. We can therefore place meaning to the expression $y = (\frac{1}{r})x$, i.e., the unique y such that $x = yr$. In a similar fashion we can attach meaning to $y = xk$ where k is an element of K. i.e, $x(\frac{r}{s}) = x(\frac{1}{s})r = yr$ if and only if $ys = x$. This makes F a vector

space over K. Therefore, we can choose a basis $\{x_i \mid i \in I\}$ of F. $F = \bigoplus_{i \in I} x_i K$ and $x_i K$ is isomorphic to K both as a K-module and as a D-module. Hence F is isomorphic to a direct sum of copies of K.

We now turn our attention to T. T is a divisible, torsion submodule of M. So T is the direct sum of primary submodules each of which is divisible. For convenience, we may assume T is, itself, a p-primary submodule. Our objective is to show that T is a direct sum of modules each isomorphic to D_p^∞. Let B represent the set of all independent sets of submodules of T isomorphic to D_p^∞. From Lemma 2.4, B is non-empty so it can be ordered by inclusion. Any chain in B, $\{L_i\}$, has an upper bound.

Subproof: I claim $\cup L_i$'s is an upper bound. We need only show that $\cup L_i$ is an element of B. Recall, a set of modules is independent if and only if each finite subset of the set is independent. If $A_1, \ldots, A_k$ is a finite subset from $\cup L_i$, then since the L_i form a chain, there is an L_j which has as members all the modules $A_1, \ldots, A_k$. But L_j is an independent set, so $A_1, \ldots, A_k$ form an independent set. This shows $\cup L_i$ is an independent set of modules. Hence $\cup L_i \in B$.

Therefore, we can apply Zorn's Lemma and get a maximal element $\{S_i\}$ of B. Let $S = \sum S_i$. I claim $S = T$. $S_i \tilde{=} D_p^\infty$ so S is the direct sum of divisible modules, hence S is divisible. By Theorem 2.2, $T = S \oplus R$. By Lemma 2.4, R must be the zero module, for if $R \neq 0$ then R contains a non-zero submodule isomorphic to D_p^∞ and adjoining this submodule to $\{S_i\}$ contradicts the maximality of $\{S_i\}$. Henct $T = S$ and our proof is complete.

Every divisible module can be uniquely specified up to isomorphism by a set of cardinal numbers, $\{\alpha_0\} \cup \{\alpha_p \mid p \in P\}$ where α_0 numbers the copies of K and for each $p \in P$, α_p numbers the copies of D_p^∞. Our conclusion is: every divisible module can be described by a set of cardinal numbers.

Definition: If M is a D-module we denote by $M_{[p]}$ the submodule of M which is the set $\{x \in M \mid xp = 0\}$.

$M_{[p]}$ is both a D and a $\frac{D}{pD}$ - module where $\frac{D}{pD}$ multiplication is defined by $m(d + pD) = md$. Multiplication is well-defined.

Proof: Let $d + pD = d' + pD$, then $(d - d') \in pD$. Let $m \in M_{[p]}$, then $m(d' + pD) = md'$ and $m(d + pD) = md$. Since $(d - d') \in pD$, then $m(d - d') = 0$. Therefore, $md - md' = 0$ or $md = md'$.

Lemma 2.6: If $M = \oplus M_i$ then $M_{[p]} = \oplus M_{i[p]}$.

Proof: Let $x \in M_{[p]}$, then $xp = 0$, but $x = \sum m_i$ and $xp = (\sum m_i)p = 0$. Therefore, $0 = \sum m_i'$ where $m_i' = m_i p \in M_i$ and since this sum is direct each $m_i' = 0$ so $m_i \in M_{i[p]}$.

Lemma 2.7: D_p^∞ is a one dimensional space over the field $\frac{D}{pD}$ with a basis $\{\frac{\bar{1}}{p}\}$.

Proof: The submodules of D_p^∞ are of the form $H_k = \{\frac{a}{p^k} \mid a \in D\}$. We note then $D_p^\infty[p] = H_1 = \frac{\bar{1}}{p} D$. Let $\phi: D \to \frac{\bar{1}}{p} D$ be defined by $\phi(x) = \frac{\bar{1}}{p} x$. Then ϕ is an epimorphism with kernel pD, by the first isomorphism theorem, $H_1 \tilde{=} \frac{D}{pD}$ as D-modules. Let λ be an isomorphism mapping H_1 to $\frac{D}{pD}$. Then $\lambda(xd) = \lambda(x)d$, and by our multiplication $\lambda(x(d + pD)) = \lambda(xd) = \lambda(x)d = \lambda(x)\ (d + pD)$ so λ is also an isomorphism of $\frac{D}{pD}$ modules.

Lemma 2.9: If p and q are distinct primes and if A is a q-primary module then $A_{[p]} = 0$.

Proof: Let $x \in A_{[p]}$, then since A is q-primary $p \in q^k D$ for some $k \geq 0$. This implies $q^k | p$, therefore $k = 0$ and x is annihilated by all of D, hence $x = 0$.

Lemma 2.10: If M_D is a divisible module and if $M = \oplus M_i$ is a decomposition of M where each M_i is a copy of D_p^∞ for some fixed prime p, then the cardinality of I, $| I |$, is the dimension of $M_{[p]}$ as a vector space over the field $\frac{D}{pD}$.

Proof: $M = \oplus_{i \in I} M_i$ implies $M_{[p]} = \oplus_{i \in I} M_{i[p]}$. But, $M_{i[p]}$ is isomorphic to D_p^∞ hence, by Lemma 2.7, is a one dimensional space over $\frac{D}{pD}$. Thus, $M_{[p]}$ is a direct sum of $| I |$ spaces of dimension one, hence $\dim_{\frac{D}{pD}} M_{[p]} = | I |$.

The above lemmas allow us to make a stronger statement than the one immediately following Theorem 2.5. Not only does a set of cardinal invariants determine up to isomorphism a divisible module, but a divisible module uniquely determines a set of cardinal invariants.

Theorem 2.11: If a divisible module M is decomposed as a direct sum of copies of the modules K_D and modules of the type D_p^∞, $p \in P$, then the numbers of the copies appearing in the decomposition is given by the formulae: $\alpha_0 = \dim_K (\frac{M}{tM})$; for $p \in P$, $\alpha_p = \dim_{\frac{D}{pD}} tM_{[p]}$. Thus these cardinal numbers are fixed once M is known, and are independent of the particular decomposition of M.

Proof: (Sketched) Let $M = \bigoplus_{i \in I} M_i$ be given where $M_i \tilde{=} D_D$ or $M_i \tilde{=} D_p^\infty$ for some $p \in P$.

(1) Let $I = I_0 \cup I_1$, where $I_0 = \{i \in I \mid M_i \tilde{=} K_D\}$ and $I_1 = I - I_0$.

(2) Then $M = F \oplus T$, where $F = \bigoplus_{i \in I_0} M_i$, $T = \bigoplus_{i \in I_1} M_i$

(3) $T = tM$. Clearly $T \subseteq tM$. It must be shown $tM \subseteq T$.

Let $x \in tM$ then $xd = 0$ for some $d \neq 0$ in D.

But $x = f + t$ where $f \in F$, $t \in T$, so

$xd = (f + t)d = fd + td = 0$. This implies $fd = td = 0$,

but for $fd = 0$ when $d \neq 0$ implies $f = 0$. Therefore,

$x = t \in T$, and $tM \subseteq T$.

(4) So, $F \tilde{=} \frac{M}{tM}$ both as a D and as a K-module. Then

$\alpha_0 = \dim_K \frac{M}{tM} = \dim_K F = |I_0|$ since $\dim_K M_i = 1$ for each $i \in I_0$

(5) Let $I_1 = \bigcup_{q \in P} I_q$ where $I_q = \{i \in I_1 \mid M_i \tilde{=} D_q^\infty\}$

(6) Then $T = \bigoplus_{q \in P} T_q$ where $T_q = \bigoplus_{i \in I_q} M_i$

(7) By the preceding lemmas:

$tM_{[p]} = T_{[p]} = \bigoplus_{q \in P} T_{q[p]} = T_{p[p]} = \bigoplus_{i \in I_p} M_{i[p]}$

(8) Hence, $\alpha_p = \dim_{\frac{D}{pD}} tM_{[p]} = \dim_{\frac{D}{pD}} (\bigoplus_{i \in I_p} M_{i[p]}) = |I_p|$.

The significance of this is that one can determine whether two divisible modules are isomorphic simply by comparing these cardinal invariants.

Example:

Are the real numbers mod the integers, $\frac{R}{Z}$, isomorphic to the complex numbers mod the gaussian integers $\frac{C}{G}$? We need only look at

the cardinal invariants to answer this question. Let $\phi: C \to R \times R$ be defined by $\phi(a+bi) = (a,b)$. Then ϕ is an isomorphism and $\phi: G \to Z \times Z$. So, $\frac{C}{G} \cong \frac{R \times R}{Z \times Z} \cong \frac{R}{Z} \times \frac{R}{Z}$. Our question can now be stated: is $\frac{R}{Z} \cong \frac{R}{Z} \times \frac{R}{Z}$? The answer is no. For any α_p of $\frac{R}{Z}$, $\alpha_p = 1$, but for α_p of $\frac{R}{Z} \times \frac{R}{Z}$, $\alpha_p = 2$.

CHAPTER III

FREE AND FINITELY GENERATED MODULES

Definition: Given a non-zero module M_D the non-empty set $B = \{b_i \mid i \in I\}$ is said to be a basis of M_D if and only if:

i) B generates M_D

ii) if $\sum b_i d_i = 0$ then each $d_i = 0$.

Definition: A module with a basis is said to be a free module

If we analyze a free module M_D in the same manner as a vector space, we must deal with the notion of "dimension." By dimension is meant the cardinality of a basis of M_D. In vector space theory this cardinality is well-defined. Is this the case for any free module over any ring? The answer in general is negative. So we must find a substitute notion for "dimension." Our procedure is the following:

Let M_D be a torsion-free D-module. Let S be the multiplicative set of non-zero elements of D. In $M \times S$, we define the relation $\sim$ by $(m_1, s_1) \sim (m_2, s_2)$ if and only if $m_1 s_2 = m_2 s_1$. Since M_D is torsion-free $\sim$ is an equivalence relation. Let $\frac{m}{s}$ be the equivalence class of (m, s) under $\sim$, and let M_S be the set of all equivalence classes. M_S has addition, $\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{m_1 s_2 + m_2 s_1}{s_1 s_2}$ making M_S an abelian group. The same process applied to the module D_D, D over itself, yields an abelian group D_S which has a multiplication multiplication $\frac{d_1}{s_1} \cdot \frac{d_2}{s_2} = \frac{d_1 d_2}{s_1 s_2}$. In fact, D_S is a ring. D_S is

just the quotient field of D, and M_S is a D_S-module where $\frac{m}{s} \cdot \frac{d_1}{s_1} = \frac{md_1}{ss_1}$.

Definition: If M_D is a torsion-free module, then rank $M_D = \dim_{D_S} M_S$.

Hence for torsion-free modules we have our substitute notion for "dimension", namely, rank. We notice the following:

(A) Every free module M_D is torsion-free.

Proof: Let x be an element of M_D where M_D is a free module with basis $B = \{b_i \mid i \in I\}$. Then $x = \sum b_i d_i$ and if $xd = 0$ for some non-zero element d in D, then $(\sum b_i d_i)d = \sum b_i d_i' = 0$ where $d_i' = d_i d$. Since $b_i \in B$, then each $d_i' = 0$, and since $d_i' = d_i d$ and $d = 0$ so $d_i = 0$. So x is the zero element and M_D is torsion-free.

(B) If F is a free module over D, then rank F is the cardinality of a basis of F.

Proof: We know rank $F = \dim_{D_S} F_S$. I claim $\phi: F \to F_S$ defined by $\phi(f) = \frac{f}{1}$ is a monomorphism which maps basis elements of F into basis elements of F_S.

Subproof:

(i) (1) $\phi(f_1 + f_2) = \frac{f_1+f_2}{1} = \frac{f_1}{1} + \frac{f_2}{1} = \phi(f_1) + \phi(f_2)$.

(2) $\phi(fd) = \frac{fd}{1} = \frac{f}{1} \cdot \frac{d}{1} = \phi(f)d$.

(3) If $\phi(f) = 0$ then $f = 0$ hence $\ker \phi = 0$.

ϕ is thus a monomorphism of D-modules.

(ii) (1) Let $B = \{b_i \mid i \in I\}$ be a basis of F.

Let $x \in F_S$, then $x = \frac{f}{s} = \sum\frac{b_i d_i}{s} = \sum\frac{b_i}{1} \cdot \frac{d_i}{x}$. Hence $\{\phi(b_i) \mid i \in I\}$ generates F_S as a D_S-module.

(2) Let $\sum\frac{b_i}{1} \cdot \frac{d_i}{s_i} = 0$. Then we can choose a common denominator so for each i we have $\frac{d_i}{s_i} = \frac{d_i'}{s}$. So, $\sum\frac{b_i}{1} \cdot \frac{d_i}{s_i} = \sum\frac{b_i d_i'}{s} = 0$.

Therefore, $\sum b_i d_i' = 0$ which implies $d_i' = 0$. Hence $\frac{d_i}{s_i} = 0$ and we have independence.

(C) If M_D is a torsion-free module and $K_D \subseteq M_D$ then rank $K \leq$ rank M.

Proof: The proof of this statement follows from the fact that K_S is a D_S-submodule of M_S.

Generally speaking, submodules of free modules are not necessarily free. For instance, let $R = \frac{Z}{4Z}$. Then R_R is a free module. $M = \{\bar{0}, \bar{2}\}$ is a submodule of R_R. M is not free.

However, if our ring is a principal ideal domain D we have the following.

Theorem 3.1: If L is a free module over D and if M is a submodule of L then M is free.

Proof: We may assume L_D is a non-zero module. Let $B = \{b_i \mid i \in I\}$ be a basis of L. I is non-empty so we can let $\leq$ represent a well-order of I. Since $L = \bigoplus_{i \in I} b_i D$ then $x \in L$ implies $x = \sum_{i \in I} b_i d_i$. We have a projection mapping $\Pi_i : L \to D$ so that $\Pi_i(x) = d_i$. We can define $L_k = \bigoplus_{i \leq k} b_i D$ and $M_k = M \cap L_k$. Then $\Pi_k(M_k) = d_k D$ for some $d_k \in D$, and we can choose $m_k \in M_k$ so that $\Pi_k(m_k) = d_k$ where $m_k = 0$ if $d_k = 0$.

Note the following:

1) $\{m_i \mid i \in I\}$ generates M.

Subproof: Let M_k' be the submodule of M_k generated by $\{m_i \mid i \leq k\}$. Then I claim that $M_k' = M_k$.

It only has to be shown that $M_k \subseteq M_k'$. If $M_k' \neq M_k$. Let k be the smallest element of I so that $M_k \neq M_k'$. We denote the smallest element of I by 0. Let $x \in M_0$. Then $x = b_0 r_0$ and $\Pi_0(x) = r_0$ where $r_0 \in d_0 D$. So $r_0 = d_0 s$ for some $s \in D$. So $x = b_0 r_0 = b_0 d_0 s$, but $b_0 d_0 = m_0$ so $x = m_0 s$. Hence $k \neq 0$.

Let $x \in M_k$, then $\Pi_k(x) \in d_k D$ so $\Pi_k(x) = d_k s$ for some $s \in D$. Now $\Pi_k(m_k) = d_k$, so $\Pi_k(x - m_k s) = d_k s - d_k s = 0$. But $x - m_k s = \sum_{j<k} m_j j$ and $x = \sum_{j<k} m_j j + m_k s$. Hence $x \in M_k'$ and $M_k' \subseteq M_k$ This contradiction shows $M_k' = M_k$ for every $k \in I$. Hence $\{m_i \mid i \in I\}$ generates M.

2) The non-zero elements of $\{m_i \mid i \in I\}$ form a basis of M.

Subproof: Since we've already shown these M_i's generate M, we need only show independence. i.e., if $\sum m_i r_i = 0$ then each $r_i = 0$ whenever $m_i \neq 0$. Since L is torsion-free if $m_i r_i = 0$ and $m_i \neq 0$ then $r_i = 0$. So, suppose $\sum m_i r_i = 0$ and some $m_i r_i \neq 0$. Let j be the largest $i \in I$ so that this is true. Then $\Pi_j(\sum m_i r_i) = \Pi_j(m_j r_j) = d_j r_j = 0$. Since $m_j r_j \neq 0$ and $m_j \neq 0$ and $d_j \neq 0$, this implies $r_j = 0$, which implies $m_j r_j = 0$. This is a contradiction. Hence all $m_i r_i = 0$ and $m_i \neq 0$ implies $r = 0$. We, therefore have independence.

Hence the non-zero elements of $\{m_i \mid i \in I\}$ form a basis of M, and by definition M is a free module.

Theorem 3.2: If L is a free module of rank n, and if M is a submodule of L of rank k, then there exists a basis $\{b_1, \ldots, b_n\}$ of L and elements $\{d_1, \ldots, d_k\}$ in D such that $d_i \mid d_{i+1}$ for $i = 1, \ldots, K-1$ and the set $\{b_1d_1, b_2, \ldots, b_kd_k\}$ is a basis of M.

Proof: Let $\Lambda = \mathrm{Hom}_D(L,D)$. If $\lambda \in \Lambda$ then $\lambda(M)$ is an ideal of D. Consider the set of all such ideals, for $\lambda \in \Lambda$. Choose a maximal member, say $\lambda_1(M) = d_1D$, is maximal among $\{\lambda(M) \mid \lambda \in \Lambda\}$ ($d_1 \neq 0$ if $M \neq 0$). We can choose a $u_1 \in M$ so that $\lambda_1(u_1) = d_1$. If $\lambda \in \Lambda$ then $\lambda(u_1) \in d_1D$.

Subproof: Let $\lambda(u_1) = d$. Then $dD + d_1D = d'D$ so there is an a and b in D so that $da + d_1b = d'$. Let $F \in \Lambda$ such that $F = \lambda a + \lambda_1 b$. Then

$$F(u_1) = (\lambda a + \lambda_1 b)u_1 = \lambda a(u_1) + \lambda_1 b(u_1)$$
$$= \lambda(u_1)\, a + \lambda(u_1)b = da + d_1b = d'.$$

So $F(M) \supseteq d'D \supseteq d_1D = \lambda_1(M)$ and because of the maximality of $\lambda_1(M)$, $F(M) = \lambda_1(M)$ and $d'D = d_1D$. Hence $\lambda(u_1) = d$ where $d \in d_1D$.

We note that $\lambda_1(M)$ is unique because it is the largest ideal of set of ideals $\{\lambda(M) \mid \lambda \in \Lambda\}$.

We may now select a basis $\{x_i \mid i \in I\}$ of L. Consider the projections Π_i of Λ with respect to this basis. All the coordinates of u_1 are in d_1D so there is a $b_1 \in L$ such that $u_1 = b_1d_1 = \lambda_1(u_1) = \lambda_1(b_1)d_1 = d_1$ so $\lambda_1(b_1) = 1$.

I claim $L = b_1D \oplus L_1$ where $L_1 = \mathrm{Ker}\ \lambda_1$.

Subproof: 1) To see that $b_1D \cap L_1 = 0$ let $x \in b_1D \cap L_1$. Then $x = b_1d$ for some $d \in D$. $\lambda_1(x) = \lambda_1(b_1d) = \lambda_1(b_1)d = d = 0$ which implies that if $x \in b_1D \cap \text{Ker } \lambda_1$ then $x = 0$.

2) To se that if $x \in L$ then $x = y + z$ where $y \in b_1D$ and $z \in L_1$ take $y = b_1\lambda_1(x)$ and $z = x - b_1\lambda_1(x)$.

Therefore, $L = b_1D \oplus L_1$ where $L_1 = \text{Ker } \lambda_1$.

I also claim that $M = b_1d_1D \oplus M_1$ where $M_1 = M \cap \text{Ker } \lambda_1$. The proof of this statement will be omitted because of its similarity to the above argument: We can conclude that b_1d_1 is an element of a basis of M. Referring back to the original statement of our theorem, we want to prove that if L is a free module of rank n and if M is a submodule of L of rank k, then there exists a basis $B = \{b_1, \ldots, b_n\}$ of L and a set of elements $d_1, \ldots, d_k$ in D so that $d_i \mid d_{i+1}$ $i = 1, \ldots, k - 1$ and $\{b_1d_1, \ldots, b_kd_k\}$ is a basis of M. Our method will be induction on $n = \text{rank } L$.

I claim the above certainly proves our statement when $n = 1$. We've shown that b_1d_1 is a basis element of M. $M = b_1d_1D \oplus M_1$ where $M_1 = M \cap \text{Ker } \lambda_1$. $M_1 = 0$ if rank $L = 1$ since rank $M_1 \leq$ rank $M - 1 \leq 0$. Thus $\{b_1d_1\}$ is a basis of M.

Now assume rank $L = n > 1$. As above $L = b_1D \oplus L_1$ and $M = b_1d_1D \oplus M_1$. Since rank $L_1 = n - 1$ and $M_1 \subseteq L_1$ the induction assumption implies that there exists a basis $\{b_2, \ldots, b_n\}$ of L_1 and elements $d_2, \ldots, d_k$ of D such that $d_i \mid d_{i+1}$ $i = 2, \ldots, k - 1$ so that $\{b_2d_2, \ldots, b_kd_k\}$ is a basis of M_1. Then $\{b_1, b_2, \ldots, b_n\}$ is a basis of L and $\{b_1d_1, b_2b_2, \ldots, b_kd_k\}$ is a basis of M. So we

need only show that $d_1 \mid d_2$ to complete our proof. Let Π be the projection from L to D with the property that $\Pi(b_2) = 1$ and $\Pi(b_i) = 0$ if $i \neq 2$. Then $\Pi(M) = d_2D$ and $d_2D \subseteq d_1D = \lambda_1(M)$. Hence $d_2 \in d_1D$ and $d_1 \mid d_2$.

This completes our proof.

Definition: A module M_D with a finite generating set is said to be a finitely generated module.

Given a module M_D generated by a set of cardinality B, then there is a free module F of rank B and an epimorphism $\phi: F \to M$.

Proof: If $\{m_i \mid i \in B\}$ is a generating set of M and F is a free module with a basis $\{b_i \mid i \in B\}$ we define an eipmorphism $\phi: F \to M$ by taking $\phi(b_i) = m_i$ for each $i \in B$.

Given a principal ideal domain D, D_D is a free module and since a direct sum of free modules is free, any module like $\coprod_{\alpha \in A} (D_D)_\alpha$ is free. If F is a free module with a basis of cardinality $\mid A \mid$, then $F \tilde{=} \coprod_{\alpha \in A} (D_D)\alpha$.

Proof: Let $B = \{b_\alpha \mid \alpha \in A\}$ be a basis of F, then if $x \in F$, $x = \sum b_\alpha d_\alpha$. The $\{d_\alpha\text{'s}\}$ is called the set of coordinates of x with respect to $\{b_\alpha \mid \alpha \in A\}$. We can let $\Psi: F \to {}_{\alpha \in A}(D_D)$ be defined by $\Psi(x) = t$ where $t \in {}_{\alpha \in A}(D_D)_\alpha$ such that $t(\alpha) = d_\alpha$. Ψ is our desired isomorphism.

Note: If F is a free module of rank $n < \infty$, then $F \tilde{=} \prod_{i=1}^{n} D$.

Let M_D be a finitely generated module generated by a set of cardinality $n < \infty$. (It is feasible that M_D may be generated by a set of cardinality $< n$). Let $F = D \times D \times \ldots \times D = D^n$. We know

there exists an epimorphism ϕ mapping F onto M. By the first isomorphism theorem, $M \cong \frac{F}{\text{Ker } \phi}$. Let $K = \text{Ker } \phi$ then K is free with rank $k \leq n$. By Theorem 3.2, there exists a basis $\{b_1, \ldots, b_n\}$ of F and a set of elements $d_1, \ldots, d_k$ in D such that $d_i \mid d_{i+1}$ for $i = 1, \ldots, k-1$ and $\{b_1d_1, \ldots, b_kd_k\}$ is a basis of K.

So $$M \cong \frac{F}{K} \cong \frac{b_1D \times b_2D \times \ldots \times b_nD}{b_1d_1D \times \ldots \times b_kd_kD} \cong \frac{D}{d_1D} \times \frac{D}{d_2D} \times \ldots \times \frac{D}{d_kD} \times \overbrace{D \times D \times \ldots \times D}^{n-k}.$$

Therefore $M = tM \oplus G$ where tM is the torsion submodule of M, $tM \cong \coprod_{i=1}^{k} \frac{d}{d_iD}$, and G is a free module of rank $n - k$. Since $G \cong \frac{M}{tM}$, G is determined up to isomorphism by M. Thus we have the following theorems.

Theorem 3.3: A finitely generated torsion-free module is free.

Definition: Rank M, where M is a finitely generated module, is rank $(\frac{M}{tM})$.

We can completely describe G by the finite cardinal rank M. Therefore, we can turn our attention to tM.

(A) If M is a finitely generated torsion module, then $M \cong \coprod_{j=1}^{k} \frac{D}{d_jD}$, where $d_1, d_2, \ldots, d_k$ are elements of D such that $d_j \mid d_{j+1}$ $j = 1, \ldots, k-1$. We will assume none of the d_js is a unit since otherwise $\frac{D}{d_jD}$ is a zero module and we would omit it.

Definition: A set of non-units $d_1, \ldots, d_k$ in D such that $d_j \mid d_{j+1}$ for $j = 1, \ldots k-1$ and so that $tM \cong \coprod_{j=1}^{k} \frac{D}{d_jD}$ is called a set of torsion invariants of M.

We may now restate (A) as follows:

Theorem 3.4: Let M_D be a finitely generated module. Then M_D has a set of torsion invariants (possibly empty) and these determine tM up to isomorphism.

From the decomposition $tM \cong \frac{D}{d_1 D} \times \ldots \times \frac{D}{d_k D}$, we can gain further decompositions by factoring each d_j into primes.

We factor $d_j = u_j p_1^{n_{1j}} p^{n_{2j}} \ldots p_t^{n_{tj}}$ where $p_1, \ldots, p_t$ are elements of P and u_j is a unit and the n_{sj}'s are integers ≥ 0 for $s = 1, \ldots, t$. Then from Theorem 1.2 we have

$$(B) \quad \frac{D}{d_j D} \tilde{=} \frac{D}{p_1^{n_{1j}} D} \times \frac{D}{p_2^{n_{2j}} D} \times \ldots \times \frac{D}{p_t^{n_{tj}} D} .$$

Then we gain further decomposition of $t(M)$ into a direct sum of primary cyclic modules.

$$\begin{aligned} tM = {} & M(p_1^{n_{11}}) \oplus M(p_1^{n_{12}}) \oplus \ldots \oplus M(p_1^{n_{1k}}) \\ & + M(p_2^{n_{21}}) \oplus M(p_2^{n_{22}}) \oplus \ldots \oplus M(p_2^{n_{2k}}) \\ & \vdots \\ & + M(p_t^{n_{t1}}) \oplus M(p_t^{n_{t2}}) \oplus \ldots \oplus M(p_t^{n_{tK}}) \\ & \quad M_k^{||} \qquad M_{k-1}^{||} \qquad\qquad M_1^{||} \end{aligned}$$

Here the summands are arranged so that the sth column from the right is the primary decomposition of $M_s \tilde{=} \frac{D}{d_s D}$. In each row since $d_i \mid d_{i+1}$, the power of the primes is non-increasing from left to right.

Since each $M(p_j^{n_{sj}})$ is isomorphic to $\frac{D}{p_j^{n_{sj}}}$ which is indecomposable, the Krull-Schmidt Theorem tells us that the non-zero

$M(p_j^{n_{sj}})$, i.e., those for which $n_{sj} > 0$, are determined up to isomorphism. Now if two modules L_D and K_D are isomorphic then $\text{ann}_D K = \text{ann}_D L$. So, the set of annihilator ideals of the non-zero $M(p_j^{n_{sj}})$'s are completely determined by M.

Definition: The set $\{p_j^{n_{sj}} \mid n_{sj} > 0\}$ are called the primary invariants of M.

We have now proved the following theorem.

Theorem 3.5: Let M_D be a finitely generated module. Then M_D has a unique set of primary invariants. These primary invariants determine tM up to isomorphism. These primary invariant are uniquely determined by M.

Since the primary invariants determine the torsion invariants up to multiplication by units (see (B) above) we have the following:

Corollary 3.6: The set of torsion invariants of M is unique up to multiplication by unit factors.

The two facts most useful to us from now on and which are apparent from the above discussion will be formally stated as corollaries.

Corollary 3.7: Let M_D be a finitely generated torsion module. Then there are non-zero cyclic modules $M_1, \ldots, M_s$ so that $M = \bigoplus_{i=1}^{s} M_i$ and $\text{ann } M_1 \supseteq \text{ann } M_2 \supseteq \cdots \supseteq \text{ann } M_s$, and in any two such decompositions of M the annihilator ideals will be the same.

Corollary 3.8: Let M_D be a finitely generated torsion module. Then there are non-zero cyclic primary submodules $N_1, \ldots, N_k$ so that

$M = \bigoplus_{j=1}^{k} N_j$, and in any two decompositions of M the ideals $\{\text{ann } N_j \mid j = 1, \ldots, k\}$ and k will be the same.

Theorem 3.9: Any two finitely generated modules are isomorphic if and only if they have the same rank and primary invariants.

Proof: ($\leftarrow$) Assume M_D and N_D have the same rank and primary invariants. Then if $M = tM \oplus F$ and $N = tN \oplus G$, then $tM \tilde{=} tN$ and $F \tilde{=} G$ so

$$\begin{array}{ccc} M & = & tM \oplus F \\ & & \| \quad \| \\ N & = & tN \oplus G \end{array}$$

Hence $M \tilde{=} N$.

($\rightarrow$) Let M_D and N_D be two finitely generated modules such that $M_D \tilde{=} N_D$. Then if $M = tM \oplus F$ and $N = tN \oplus G$, then $tM \tilde{=} tN$. Thus by Theorem 3.5 M and N have the same primary invariants. Now if ϕ is our isomorphism $\phi: M \to N$ and f is an element of F, $\phi(f) = x + g$ where $x \in tN$ and $g \in G$. There is a $\Pi: tN \oplus G \to G$ defined by $\Pi(x + g) = g$. So $\Pi\phi: F \to G$, and $\Pi\phi$ is an isomorphism, hence M and N have the same rank.

Corollary 3.10: Any two finitely generated modules are isomorphic if and only if they have the same rank and torsion invariants.

CHAPTER IV

CANONICAL FORMS

Let V_K be a vector space of dimension n over a field K. Let λ be an element of $\mathrm{Hom}_K(V,V)$. Then V becomes a K[x]-module V_λ, where for $p(x) \in K[x]$, $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots a_0$, and $v \in V$ we define

$$p(x) \cdot v = (a_n\lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_0\lambda^0) \cdot v =$$

$$a_n\lambda^n v + a_{n-1}\lambda^{n-1}v + \ldots + a_0 v.$$

Definition: A polynomial p(x) of degree k is said to be monic if the coefficient of x^k is 1.

Definition: The ideal ann V_λ of K[x] has a unique monic genera generator q(x) called the minimal polynomial of λ.

Definition: If W is a K[x] submodule of V_λ, then the unique monic generator of the ideal ann W is called the minimal polynomial of the restriction of λ to W, denoted the minimal polynomial of $\lambda|_W$.

Investigating V_λ, we notice the following: (i) V_λ is a finitely generated K[x]-module, and (ii) V_λ is a torsion K[x]-module.

Proof: i) A generating set for V_K is also a generating set for V_λ. V_K is finitely generated, hence so is V_λ.

ii) Let a be a torsion free element of V_λ. Let [a] represent the K[x] submodule of V_λ generated by a. By Theorem 2.5, [a] is isomorphic to K[x]. K[x] has infinite dimension, so [a]

has infinite dimension. Now, V_K has a subspace [a], and this V_K has a subspace of infinite dimension. This contradicts the supposition that V_K has dimension n, hence no such a can exist, and every element of V_λ is torsion.

So, given a vector space V of dimension n over a field K together with a linear mapping λ of V into itself one can produce V_λ, which is a finitely generated torsion module over the principal ideal domain K[x].

Further investigation of V_λ gives us the following:

i) W is a K[x] submodule of V_λ if and only if W is an invariant subspace of V_K under λ. By invariant, is meant $\lambda(W) \subseteq W$.

Proof: ($\rightarrow$) Let W be a K[x] submodule of V_λ. Let $w \in W$, then $x \cdot w = \lambda(w) = w'$ where $w' \in W$. Hence W is an invariant subspace of V_K under λ.

($\leftarrow$) Let W be an invariant subspace of V_K under λ. Let $p(x) \in K[x]$. Then $p(x) = a_k\lambda^k + a_{k\ 1}\lambda^{k-1} + \ldots + a_0$. Then if $w_0 \in W$,

$$p(x) \cdot w_0 = (a_k\lambda^k + a_{k-1}\lambda^{k-1} + \ldots + a_0) \cdot w_0 =$$

$$a_k\lambda^k w_0 + a_{k-1}\lambda^{k-1}w_0 + \ldots + a_0w_0 =$$

$$a_k\lambda^{k-1}(\lambda w_0) + a_{k-1}\lambda^{k-2}(\lambda w_0) + \ldots + a_1\lambda w_0 + a_0w_0 =$$

$$a_k\lambda^{k-1}w_1 + a_{k-1}\lambda^{k-2}w_1 + \ldots + a_1w_1 + a_0w_0 \quad \text{for } \lambda w_0 = w_1 =$$

$$a_k\lambda^{k-2}(\lambda w_1) + a_{k-1}\lambda^{k-3}(\lambda w_1) + \ldots + a_1w_1 + a_0w_0 =$$

$$a_k\lambda^{k-2}w_2 + \ldots + a_2w_2 + a_1w_1 + a_0w_0 \quad \text{where } \lambda w_1 = w_2 \text{ etc.}$$

Then $p(x) \cdot w_0 \in W$. Hence W is a K[x] submodule of V_λ.

ii) W is a cyclic K[x] submodule of V_λ if and only if there is a vector $v \in W$ so that $\{v, \lambda(v), \ldots, \lambda^{k-1}(v)\}$ is a basis of W as a subspace for some non-necative integer k.

Proof: ($\rightarrow$) Let W be a cyclic $K[x]$ submodule of V_λ. Let w_0 generate W. Let $q(x)$ be the minimal polynomial of $\lambda|_W$, where $q(x) = x^k + a_{k-1}x^{k-1} + \ldots + a_1x + a_0$.

I claim $\{w_0, \lambda w_0, \ldots, \lambda^{k-1}w_0\}$ is a basis of W.

Subproof: a) Since w_0 generates W, then ann w_0 = ann W. If $p(x) \cdot w_0 = 0$ then $q(x) \mid p(x)$. Let $\sum_{j=0}^{k-1} b_j\lambda^j w_0 = 0$. Then $(b_0 + b_1\lambda + \ldots + b_{k-1}\lambda^{k-1})w_0 = 0$, so $(b_0 + b_1x + \ldots + b_{k-1}x^{k-1})w_0 = 0$. Since this polynomial has degree less than k and is a multiple of $q(x)$, it is the zero polynomial. Hence each $b_j = 0$ for $j = 0, \ldots, k-1$. Thus $\{w_0, \lambda w_0, \ldots, \lambda^{k-1}w_0\}$ is an independent set.

b) Let $w \in W$. Then $w = p(x)w_0$. I claim there exists a polynomial $r(x)$ of deg $\leq k-1$ so that $r(x)w_0 = w$. To see this we use the division algorithm. $p(x) = q(x)s(x) + r(x)$ where $r(x)$ has deg $\leq k-1$. So,

$$\begin{aligned} w = p(x)w_0 &= [q(x)s(x) + r(x)]w_0 = [s(x)q(x) + r(x)]w_0 \\ &= [s(x)[q(x)]w_0 + r(x)w_0 = s(x)[q(x)w_0] + r(x)w_0 \\ &= r(x)w_0. \end{aligned}$$

Let $r(x) = c_0 + c_1x + \ldots + c_{k-1}x^{k-1}$. Then

$$\begin{aligned} w = r(x)w_0 &= (c_0 + c_1\lambda + \ldots + c_{k-1}\lambda^{k-1})w_0 \\ &= c_0w_0 + c_1\lambda w_0 + \ldots + c_{k-1}\lambda^{k-1}w_0. \end{aligned}$$

Hence $\{w_0, \lambda w_0, \ldots, \lambda^{k-1}w_0\}$ generates W.

c) Parts a & b combine to tell us $\{w_0, \lambda w_0, \ldots, \lambda^{k-1}w_0\}$ is a basis of W_K.

As is well known, the fixing of an ordered basis B of the vector space V produces an isomorphism between $\mathrm{Hom}_K(V,V)$ and the

K-algebra of $n \times n$ matrices with entries in K. Corresponding to $\lambda \in \mathrm{Hom}_K(V,V)$ we have the $n \times n$ matrix whose i^{th} row is the ordered set of coordinates of the image of the i^{th} basis vector under λ. For a fixed λ, different matrices arise by varying the choice of the ordered basis chosen on V.

Definition: Two matrices are said to be similar if they represent the same $\lambda \in \mathrm{Hom}_K(V,V)$ by varying the choice of the ordered basis chosen on V.

Definition: An $n \times n$ matrix is said to be block diagonal if it can be partitioned so that it is a diagonal matrix of matrices where the matrices occupying the diagonal are square.

For $\lambda \in \mathrm{Hom}_K(V,V)$ and a basis B of V, it is clear that the corresponding matrix is block diagonal with blocks of dimension $n_1, n_2, \ldots, n_s$ where $\sum_{i=1}^{s} n_1 = n$ precisely when the basis B is segmented with segments of length n_i so that each segment generates a K-subspace V_i of V which is invariant under λ. Then the i^{th} block is the matrix representation of $\lambda|V_i$ for the appropriate segment of B which generates V_i as a K-subspace of V. That is, if A (the matrix representation of $\lambda \in \mathrm{Hom}_K(V,V)$ for an ordered basis B) is a block diagonal matrix, then each matrix occupying the diagonal of A indicates the existence of a subspace of V invariant under λ. And, if the ordered basis B of B can be appropriately segmented, so that each segment generates a K-space of V which is invariant under λ, then the matrix representation of λ will be a block diagonal matrix.

Now, if W is a cyclic $K[x]$ submodule of V_λ, then there is a basis of the form $\{w_0, \lambda w_0, \ldots \lambda^{k-1}w_0\}$ where w_0 generates W_λ and the degree of the minimal polynomial of $\lambda|_W$ is k. Knowing the minimal polynomial of $\lambda|_W$ we can look at a matrix representation of $\lambda|_W$ with respect to the above basis. For instance if the minimal polynomial of $\lambda|_W$ is $q(x) = x^k + a_{k-1}x^{k-1} + a_1x + a_0$ then we have the following:

$$\begin{aligned}
&\lambda(w_0) = \lambda(w_0) && \text{which has coordinates} && (0,1,0,\ldots,0)\\
&\lambda(\lambda w_0) = \lambda^2(w_0) && && (0,0,1,0,\ldots,0)\\
&\quad\vdots && \quad\vdots && \quad\vdots\\
&\lambda(\lambda^{k-1}w_0) = \lambda^k w_0 = && && \\
&-a_0w_0 = a_1\lambda w_0 - \ldots - a_{k-1}\lambda^{k-1}w_0 && && (-a_0,-a_1, \ldots, -a_{k-1})
\end{aligned}$$

giving us the $k \times k$ matrix of the form:

$$\begin{pmatrix}
0 & 1 & 0 & \cdots & 0\\
0 & 0 & 1 & 0 & \cdots & 0\\
 & & & \ddots & & 0\\
 & & & & \ddots & 1\\
-a_0 & -a_1 & & \cdots & & -a_{k-1}
\end{pmatrix}$$

Definition: The above matrix is called the companion matrix of $q(x)$, where $q(x)$ is the minimal polynomial of $\lambda|_W$.

Thus if W is an invariant subspace then W is a cyclic $K[x]$ submodule if and only if $\lambda|_W$ has a companion matrix representation for some ordered basis of W.

Now, since V_λ is a finitely generated torsion module over the principal ideal domain $K[x]$, Corollary 3.7 tells us V_λ decomposes into a direct sum of non-zero, torsion, cyclic $K[x]$ submodules, $V = V_1 \oplus \ldots \oplus V_s$ where ann $V_1 \supseteq$ ann $V_2 \supseteq \ldots \supseteq$ ann V_s. Since each V_i is a non-zero cyclic $K[x]$ submodule there exists a set of generators $\{v_i\}$, $i = 1, \ldots, s$, so that $\{v_1, \lambda v_1 \ldots, \lambda^{k_1-1} v_1\}$ is a basis of V_1, $\{v_2, \lambda v_2, \ldots, \lambda^{k_2-1} v_2\}$ is a basis of V_2 and, in general, $\{v_i, \lambda v_i, \ldots, \lambda^{k_i-1} v_i\}$ is a basis of V_i for $i = 1, \ldots, s$. Hence V_λ has a (segmented) basis of the form:

$$\{v_1, \lambda v_1, \ldots, \lambda^{k_1-1}; v_1; v_2, \lambda v_2, \ldots, \lambda^{k_2-1} v_2; \ldots; v_s, \lambda v_s, \ldots, \lambda^{k_s-1} v_s\}$$

where $\sum_{i=1}^{s} k_i = n$ and k_i is the degree of the minimal polynomial of $\lambda|_{V_i}$. Our discussion of block diagonal matrices tells us the matrix representation of λ with respect to the above ordered basis will be a block diagonal matrix. If we let Q_i represent the i^{th} block of our block diagonal matrix representation, we see Q_i will be the companion matrix of the minimal polynomial of $\lambda|_{V_i}$. And the matrix representation of λ with respect to the above ordered basis is of the form:

$$\begin{pmatrix} Q_1 & & 0 \\ & \ddots & \\ & \ddots & \\ 0 & & Q_s \end{pmatrix} = R$$

where Q_i is a $k_i \times k_i$ matrix $i = 1, 2, \ldots, s$ and if $q_i(x)$ is the minimal polynomial of $\lambda|_{V_i}$ then $q_i \mid q_{i+1}$ for $i = 1, \ldots, s - 1$.

Corollary 3.7 tells us that this matrix is uniquely determined, because the minimal polynomials of the annihilator ideals in our decomposition are uniquely determined.

Definition: A matrix having the same form as the above matrix is said to be in Rational Canonical Form.

So, if A is any $n \times n$ matrix over K we can let V be the space of n-tuples of elements of K and let $\lambda \in \mathrm{Hom}_K(V,V)$ be defined by $\lambda(v) = v \cdot A$. By choosing the ordered basis $B_1 = \{\epsilon_i \mid i = 1 \ldots n\}$ where ϵ_i is the i^{th} row of the identity matrix then, with respec to the basis B_i, λ is represented by A itself. But, by Corollary 3.7 and prior discussion there is another basis B_2 for V, so that λ is represented by a unique matrix R in Rational Canonical Form. A and R are similar by definition. The above discussion gives us the following:

Theorem 4.1: Let A be an $n \times n$ matrix over K, then A is similar to a unique matrix in Rational Canonical Form.

Definition: A field F is said to be algebraically closed if every polynomial in $F[x]$ of degree greater than one factors into linear factors.

Let W be a primary cyclic $K[x]$ submodule of V_λ, where K is an algebraically closed field. Let $p(x)$ be the minimal polynomial of $\lambda|_W$. Because K is algebraically closed field a polynomial is prime if and only if it has degree one and since p is primary, $p(x) = (x-a)^k$ for some $a \in K$. Now, there exists a $w_0 \in W$ so that $W = w_0K[x]$ and there is an isomorphism so that $w_0K[x] \tilde{=} \frac{K[x]}{p(x)\ K[x]}$

both as a $K[x]$ module and as a K-space. I claim that as a K-space the cosets $\{\bar{1}, \overline{(x-a)}, \ldots, \overline{(x-a)}^{k-1}\}$ form a basis of $\frac{K[x]}{p(x)\ K[x]}$.

Proof: i) Let $\sum_{j=0}^{k-1} b_j \overline{(x-a)}^j = \bar{0}$. Then

$b_0\ \bar{1} + b_1\overline{(x-a)} + \ldots + b_{k-1}\overline{(x-a)}^{k-1} = \bar{0}$, that is

$b_0 + b_1(x-a) + \ldots + b_{k-1}(x-a)^{k-1} = \bar{0}$. Which means

$p(x) \mid (b_0 + b_1(x-a) + \ldots + b_{k-1}(x-a)^{k-1})$. But $p(x)$ is of k^{th} degree so $b_0 + b_1(x-a) + \ldots + b_{k-1}(x-a)^{k-1}$ must be the zero polynomial. Hence each $b_j = 0$, and we have independence.

ii) Given a coset $\overline{f(x)}$ of $\frac{K[x]}{p(x)\ K[x]}$, we may assume $f(x)$ has degree less than k, because by the division algorithm $f(x) = p(x) \cdot u(x) + r(x)$ where $r(x)$ has degree $\leq k - 1$. So $\overline{f(x)} = \overline{r(x)}$, and $r(x)$ can be expressed as $c_0 + c_1(x-a) + \ldots + c_{k-1}(x-a)^{k-1}$ where each c_j for $j = 0, \ldots, k-1$ is uniquely determined. Hence $\overline{f(x)} = c_0\ \bar{1} + c_1\overline{(x-a)} + \ldots + c_{k-1}\overline{(x-a)}^{k-1}$. So, $\bar{1}, \overline{(x-a)}, \ldots, \overline{(x-a)}^{k-1}$ generates $\frac{K[x]}{p(x)\ K[x]}$.

iii) Parts i) and ii) combine to show that $\{\bar{1}, \overline{(x-a)}, \ldots, \overline{(x-a)}^{k-1}\}$ is a basis of $\frac{K[x]}{p(x)\ K[x]}$.

The isomorphism $\phi: \frac{K[x]}{p(x)\ K[x]} \to W$ is defined by $\phi(\overline{f(x)}) = f(x) \cdot w_0$. So by way of this isomorphism, the set $B = \{w_0, (\lambda-a)^{k-1}w_0, \ldots, (\lambda-a)^{k-1}w_0\}$ forms a basis of W over K. Knowing the minimal polynomial of $\lambda|_W$, $p(x) = (x-a)^k$ we may look at a matrix representation of $\lambda|_W$ with respect to this basis.

Noting that $\lambda(\lambda-a)^\ell = a(\lambda-a)^\ell + (\lambda-a)^{\ell+1}$ then:

$\lambda(w_0) = aw_0 + (\lambda-a)w_0$ has coordinates $(a,1,0,\ldots,0)$

$\lambda(\lambda-a)w_0 = a(\lambda-a)w_0 + (\lambda-a)^2 w_0$ $(0,a,1,0,\ldots,0)$

$\vdots$

$\lambda(\lambda-a)^{k-1}w_0 = a(\lambda-a)^{k-1}w_0 (\lambda-a)^k w_0 = a(\lambda-a)^{k-1}$ $(0,\ldots\ldots 0,a)$

Then with respect to the basis B the mapping $\lambda|_W$ has the matrix representation:

$$\begin{pmatrix} a & 1 & 0 & \cdot & \cdot & 0 \\ 0 & a & 1 & 0 & \cdot & 0 \\ & & \ddots & \ddots & \ddots & \\ & & & & 0 & \\ & & & & & 1 \\ & & 0 & & & a \end{pmatrix}_{k \times k}$$

Definition: The above matrix is called the Jordan Block of $p(x) = (x-a)^k$.

Thus we see that if W is an invariant subspace then W is a primary cyclic K[x] submodule if and only if $\lambda|_W$ has a Jordan Block matrix representation for some ordered basis of W.

Now, since V_λ is a finitely generated torsion module over a principal ideal domain, Corollary 3.8 tells us that V_λ decomposes into a direct sum of primary cyclic K[x] submodules, this decomposition is unique up to order. $V_\lambda = V_1 \oplus \ldots \oplus V_t$. Since each V_i, $i = 1, \ldots, t$ is a primary cyclic K[x] submodule there exists a set of elements $\{v_i \in V_i \mid i = 1, \ldots, t\}$ and $\{a_i \in K \mid i = 1, \ldots, t\}$ so that $\{v_1, (\lambda-a_1)v_1, \ldots, (\lambda-a_1)^{k_1-1}v_1\}$ is a basis of V_1, $\{v_2, (\lambda-a_2)v_2, \ldots, (\lambda-a_2)^{k_2-1}v_2\}$ is a basis of V_2,

and in general $\{v_i, (\lambda-a_i)\, v_i, \ldots, (\lambda-a_i)^{k_i-1} v_i\}$ is a basis of V_i. Hence V_λ has a (segmented) basis of the form $\{v_1,(\lambda-a_1)v_1,\ldots,(\lambda-a_1)^{k_1-1} v_1; \ldots; v_t,(\lambda-a_t)v_t,\ldots,(\lambda-a_t)^{k_t-1} v_t\}$ where $\sum_{i=1}^{t} k_i = n$ and k_i is the degree of the minimal polynomial of $\lambda|_{V_i}$. Our discussion of block diagonal matrices tells us the the matrix representation of λ with respect to the above ordered basis will be a block diagonal matrix. If J_i represents the i^{th} block of our block diagonal matrix representation, we see J_i will be the Jordan Block of the minimal polynomial of $\lambda|_{V_i}$. The matrix representation of λ with respect to the above ordered basis is of the form:

$$\begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_t \end{pmatrix}_{n \times n}$$

where J_i is the Jordan block of the minimal polynomial of $\lambda|_{V_i}$.

Definition: A matrix of the above form is said to be in Jordan canonical form.

So, using the same argument as used in demonstrating that a matix is similar to a matrix in Rational Form, and Corollary 3.8, we have the following:

Theorem 4.2: Let A be an $n \times n$ matrix over an algebraically closed field K, then A is similar to a matrix in Jordan form. The matrix in Jordan form is unique up to the order in which the Jordan blocks are arranged on the diagonal.

CHAPTER V

SUMMARY

It has been shown that if a divisible module M_D is decomposed into a direct sum of submodules, then each submodule is isomorphic to a product of copies of the module K_D and modules of the type D_{p^∞}. No matter how M_D is decomposed as a direct sum of submodules, the numbers of copies of K_D and D_{p^∞} for various primes $p \in P$ remain fixed. This set of numbers is called the set of cardinal invariants and serves to determine the module up to isomorphism.

Also, it has been shown that any finitely generated module M_D decomposes into a direct sum of the torsion submodule tM and a torsion-free submodule F isomorphic to $\frac{M}{tM}$. The torsion submodule is a finite product of cyclic modules. There is a canonical decomposition of this type such that the generators of these cyclic modules uniquely determine a set of elements in D called the set of torsion invariants. The torsion-free submodule is a finite product of copies of D. The number of these copies is called the rank of M. Again the rank of M and the torsion invariants of M serve to determine M up to isomorphism.

Furthermore, given a vector space of finite dimension over a field K and a linear mapping λ of V into itself one can produce V_λ which is a finitely generated torsion module over the principal ideal domain $K[x]$. The torsion invariants of V_λ determine a segmented basis of V which uniquely determines a matrix representation of λ in Rational canonical form. If K is an algebraically closed field,

the primary invariants of V_λ determine a segmented basis which determines a matrix representation of λ in Jordan canonical form. This representation is unique up to the ordering of its Jordan blocks.

BIBLIOGRAPHY

1. Irving Kaplansky, Infinite Abelian Groups, The University of Michigan Press, Ann Arbor, Michigan, 1969.

2. Joachim Lambek, Lectures on Rings and Modules, Blaisdell Publishing Company, Waltham, Massachusetts, 1966.